

# Physical Red Teaming for Cyber Security Teams

Ana Aslanishvili & Shawn Abelson

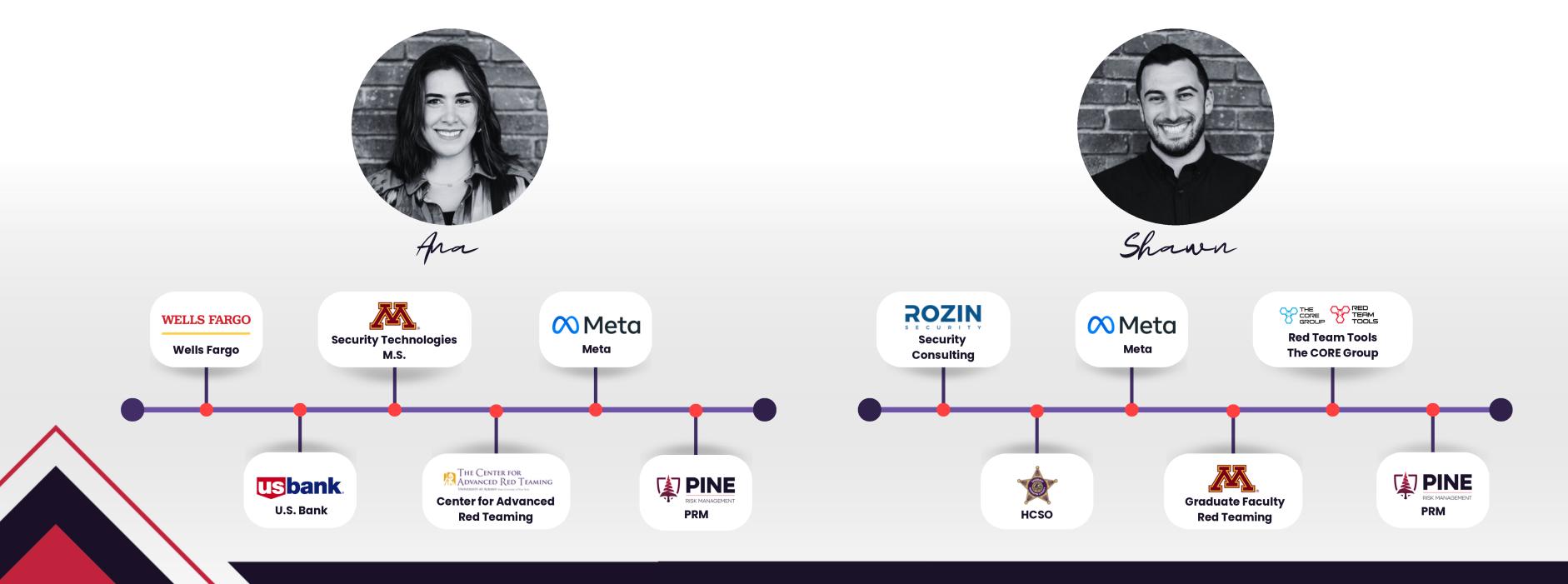
# Agenda

- Physical Security Primer for Cybersecurity Professionals
- Physical Red Teaming (PRT)
- PRT Approaches for Cybersecurity Teams
  - Similarities & Differences
- PRT Lifecycle
- Common Pitfalls of PRT (Learn from Our Mistakes)
  - Red Teams Gone Wild
- Becoming a Good Physical Red Teamer
- How to Run Physical Red Teams
- Contributing to the Profession
- Resources



## **About Us**

**PRM**: We conduct, build, and train red teams, helping organizations mature and improve security. **Meta**: Started largest physical red team in Silicon Valley, hired dozens of testers, and built a team to oversee findings remediation across global office and data center footprint.



# Physical Security @ Def Con

- 8/8: Red Team Alliance's Red Team Rendezvous
- 8/9: High Intensity Deconstruction: Chronicles of a Cryptographic Heist
- 8/9: Badge Cloning: A Penetration Tester's Guide to Capturing and Writing Badges
- 8/9: Physical Security Bypassing Access Control Systems
- 8/9: Optical Espionage: Using Lasers to Hear Keystrokes Through Glass Windows
- 8/9: Master Splinter's initial physical access dojo: Storytelling of a complex adversarial
- 8/10: Physical Red Teaming for Offensive Cyber Teams
- 8/10: Improv and social engineering for red teamers
- 8/11: Physical OSINT
- 8/11: Fitness of Physical Red Teamers











# **Physical Security**

Protecting People, Assets, and Reputation. Security measures that deny unauthorized access to facilities, equipment, and resources and to protect personnel and property from damage or harm.



## Components of Physical Security

Physical: Doors, locks, gates, bollards, etc.

**Technology:** PACS, CCTV, Radios, Investigative, and Intelligence tools

**Human:** Guards, Analysts, Managers, Awareness, Processes & Procedures



# Physical Security

# Physical Security Teams & Activities





Threat Management



Event Security



Travel Safety



Business Continuity



Systems and Design



Quality Assurance



GSOC



**Red Team** 



Investigations



Intellectual
Property Protection



Supply Chain Security



Security Awareness



Insider threat management



Guard-force management



Governance, Risk, and Compliance



Audit



Protective Design



Resilience



Protective Intelligence



Executive Protection



# **Physical Security**

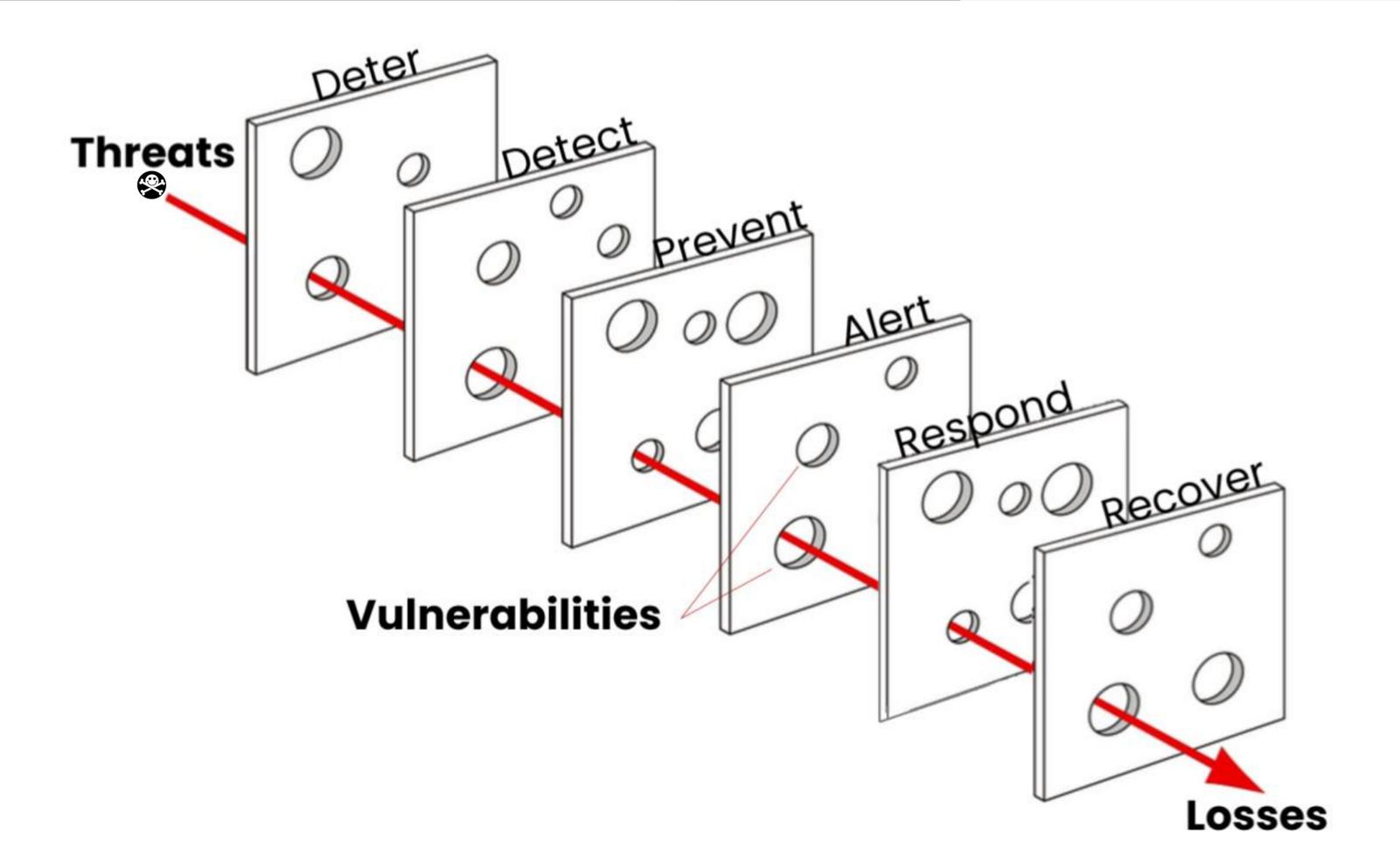
Goals of Physical Security















# The Profession of Physical Security

AMBIGUOUS BORDERS

VARIABLE REPORTING STRUCTURES

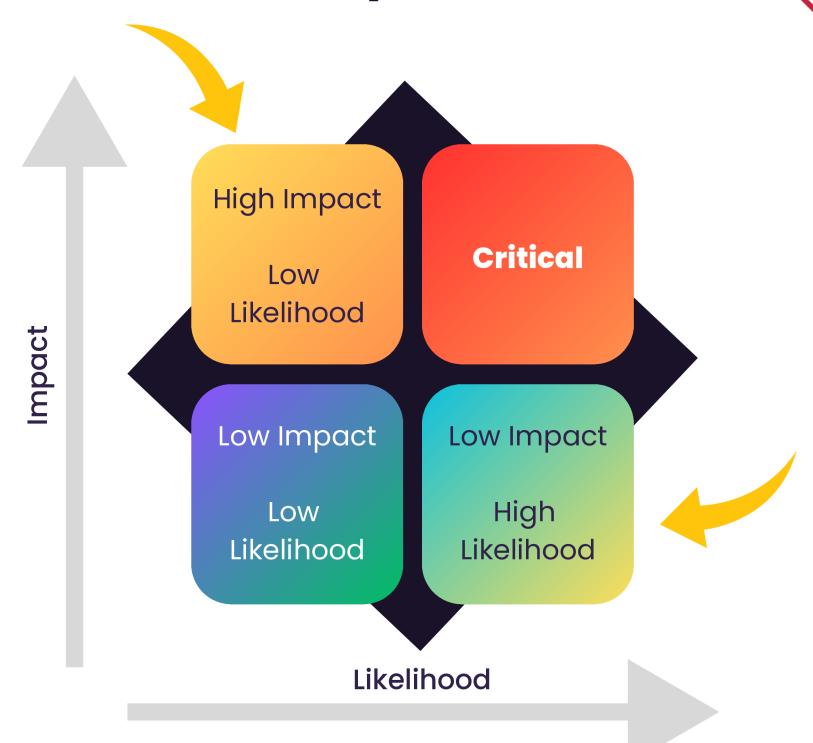
HIERARCHICAL

IMMATURE

SLOW

IRREGULAR

ASYMMETRIC





# **Testing Physical Security**

## PHYSICAL SECURITY COVERS A WIDE ARRAY OF THREATS WITH A LIMITED BUDGET.

Infosec conducting Physical Security testing can result in a undue and overwhelming focus on technology and physical measures protecting IT infrastructure.

**Example:** Your testing may trigger a million dollar remediation project to replace Wiegand with OSDP, when in reality the likelihood of a badge being cloned is dramatically lower than that of workplace violence (domestic violence) or insider threat.

Some security programs are immature and need the help.
Many are not and are drowning in data, threats, vulnerabilities, and more.

((( ))) Before you test, know how you will contribute to the status quo and prioritization.

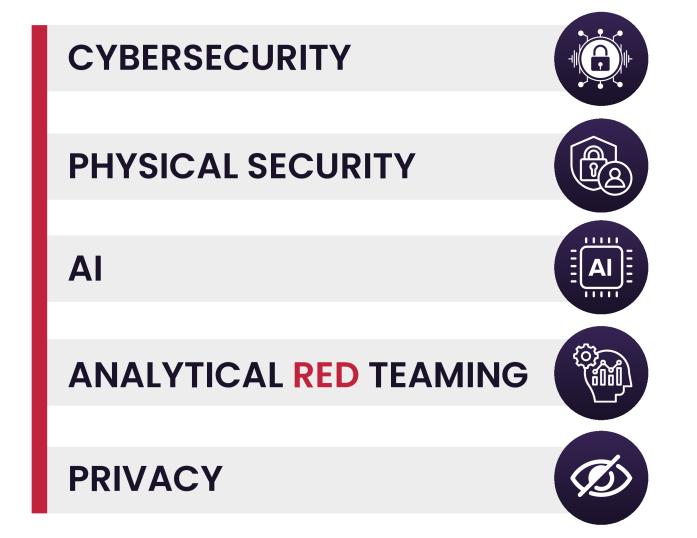


# Define Red Teaming

Stress Testing: Testing a system with the goal to improve it



## Types of Red Teams



## Types of Assessments

ASSET FOCUSED ASSESSMENT



VULNERABILITY FOCUSED ASSESSMENT



THREAT FOCUSED ASSESSMENT



# Define Red Teaming

## WHAT'S THE POINT?

The Red Team as a Blue Team in disguise.

Red Team findings help the Blue Team prioritize the endless litany of tasks, fixes, and remediations they need to accomplish - driven by the same purpose behind the mission.

Threat-Centric Risk Framework **Focus:** Profiles probable attackers and their likely methods of attack.

Approach: Identifies avenues of attack and the targeted hardware/software.

Figure out who will target you, put yourself in their shoes and figure out their target: TTPs, vulnerabilities they may exploit, etc.

Vulnerability-Centric Risk Framework **Focus**: Identifies security vulnerabilities within the system.

**Approach:** Quantifies the criticality of each vulnerability.

Testing of specific controls to validate strength, identify weaknesses, and improve capabilities.
Pen Testing.

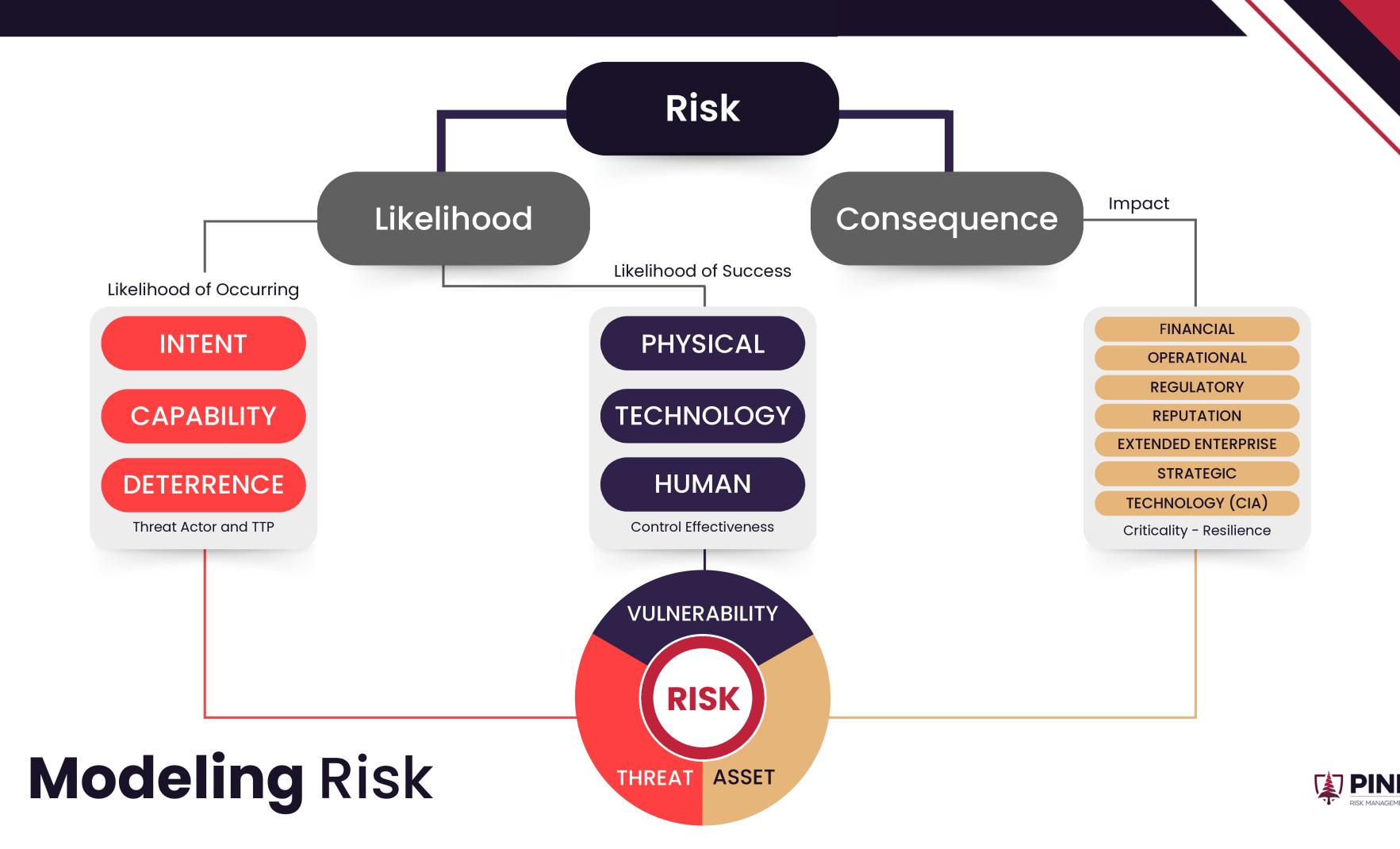
Asset-Centric Risk Framework Focus: Identifies and prioritizes risks based on system assets.

**Approach**: Evaluates the business impact of losing each asset.

Identify the business's goals, and the most important assets that enable those goals to succeed.

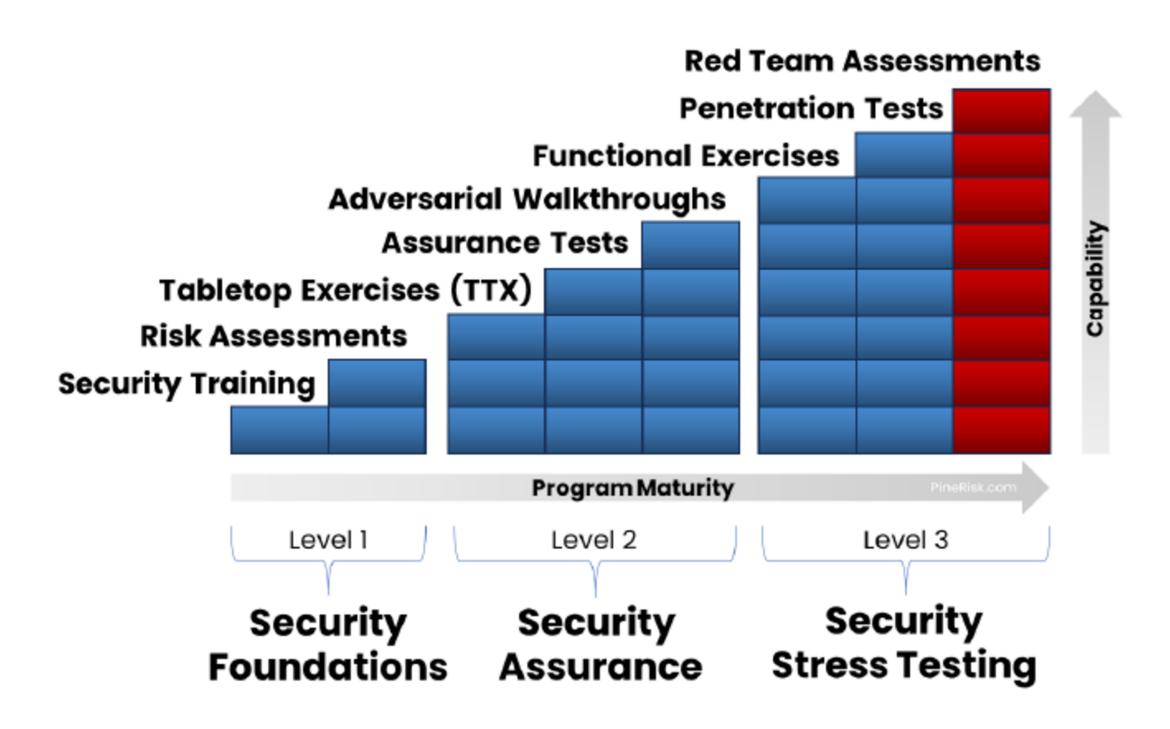
Steal the Assets.





# Physical Red Teaming

## Security Maturity Spectrum





# Why are Cybersecurity teams testing Physical Security?





Cyber teams testing
whether physical
security creates cyber
weaknesses



Cyber teams testing physical because it's fun & interesting



Cyber teams partnering with physical to help improve physical programs



Cyber teams testing physical as part of a requirement (certification or regulatory)



# Approach: Team Makeup

## WHAT TYPE OF TEST ARE YOU RUNNING?

Physical Enabled
Cyber



Full Physical Assessment



Cyber with a Twist



Test Specific
Physical Controls



Test Physical
Security Technology





# **Benefits of Testing Physical Security**

## Breakdown Boundaries / Silos

• Don't give the adversary an advantage

Increased Collaboration between Physical / Cyber

Holistic View of Company's Security Risks

**Better Assessments** 

**Unassigned Areas of Responsibility** 

- Fiber-tapping
- Vendor Onboarding
- Insider Threat





# Similarities in Testing

Approach – Adversary emulation / stress testing Need for OpSec Blue teamer in disguise Kill-Chain

Security Objective	Prevent ▼		Security Component	Human ▼		Security Layer	Roof Access						
Recon	Surveillance	Resource Development	Probing	Pretexting	Perimeter Breach	Facility Breach	Persistance	Privledge Escalation	Defense Evasion	Discovery	Collection	Exfiltration	Impact
54 Techniques	17 Techniques	22 Techniques	44 Techniques	33 Techniques	37 Techniques	44 Techniques	52 Techniques	26 Techniques	32 Techniques	34 Techniques	46 Techniques	48 Techniques	54 Techniques
OSINT	Identify Security Measures	Impersonation	Testing physical barriers and locks	Posing as maintenance or repair personnel	Climbing fences or visits	Using stolen or counterfeit access cards	Creating hidden compartments within the facility	Using stolen or forged credentials	Disabling security cameras or alarms	Mapping out security camera locations	Gathering sensitive documents or data	Smuggling documents or data out of the facility	Destroying physical security systems or barriers
Linkedin Employee Search	Individual: Static Surveillance (sitting on bench or coffee shop nearby)	Purchase Clothing	Altempting to access restricted areas	Using fake identities to gain information	Cutting through barriers or fencing	Taigating authorized personnel into buildings	Installing covert surveillance equipment	Exploiting software vulnerabilities	Using counterfeit identification	Identifying access control points	Recording audio or video of sensitive areas	Using encrypted communication channels	Tampening with ortical infrastructure
Geogre Dorking	Individual: Dynamic Surveillance (natking around)	Print Lookalike Badges (BASED ON: OSINT of current employees)	Triggering alarms to observe response times	Prefending to be a new employee	Using vehicles to ram gates or partiers	Posing as cleaning or maintenance staff	Planting devices that can be remotely accessed	Manipulating access control systems	Exasing or manipulating logs	Surveying internal layout of the facility	Using covert cameras or recording devices	Transferring data to external storage devices	Disrupting power or communication tines
Recent News/Media	Vehicle-Based Surveillance		Conducting false maintenance requests  Checking for unsecured doors or	Creating fictitious scenarios to elicit information Impersonating delivery or service	Exploiting gaps or vealinesses in feecing Using ladders or other tools to	Forcing doors or windows open Bypassing electronic access	Establishing recurdant access points	Using social engineering to gain higher privileges	Disguising as authorized personnel	Gathering employee shift schedules	Collecting access credentials and bedges Harvesting information from	Sending data via email or file sharing senices Using remote access tools for data	Initiating fire or smoke to cause evacuations Damaping key assets or
Localized Image Search	Handheld Photography	Breach Tool Acquisition	vindovs	impersonating delivery or service vioriters	Using ladders or other tools to scale obstacles	control systems	Using social engineering to maintain access	Installing backdoors or roofkits	detection	Identifying key personnel and their routines	snicked computers	Using remote access tools for data transfer	comaging key assets or equipment
	Covery Persistent Photography	tools based on site hardware (e.g. Link, plox gun, bar bypass)	Using social engineering to gather access information	Posing as law enforcement or government officials	Digging tunnels or trenches to bypass barriers	Exploiting HVAC or utility access points	Hiding in seldors-used areas of the facility	Compromising administrator accounts	Using encryption to hide activities	Investigating security protocols and response times	Obtaining data from printers or copiers	or images	Compromising data integrity or availability
Obtain Facility Layout	Sensor Placement		Attempting to bypass security systems	trust	Cisabling perimeter alarms or sensors	Using hidden compartments to smuggle tools	Setting up temporary camps or stations	Utilizing insider threats or collusion	Deploying decoys or distractions	Analyzing entry and exit logs	Collecting discarded documents from trash or recycling	Uploading data to cloud storage services	Introducing malurare or ransormulare
City construction permits		Bypass Tool Acquisition	Observing and testing security personnel reactions Testing access control systems	Calling with ungent requests for information  Sending emails with fabricated	Taligating authorized personnel through gates  Using fale credentials to pass	Descrivating alarm systems and sensors Cloring access badges or	Compromising junitorial or utility closets  Using false maintenance requests	Exploiting default passwords or settings  Leveraging trust relationships between	Avoiding security patrol routes	Searching for unmonitored or less-secured areas	Copying files from network shares or servers Using USS serves or other portable	Using physical drop points for data exchange Sending data through secure	Manipulating environmental controls (e.g., HVWC) Sabolaging network or IT
City blueprints	Identify Vendors	tool, and other typess tools.  Create mock up of target site using	with fake credentials	stories	through checkpoints	keycards	to stay onsite	systems	techniques	assets	storage devices	turnets or VPTI's	infrastructure
Landland rental site	Using drones to monitor the facility Monitoring employee and visitor patterns	surveillance and CSRIT rate	Using social engineering to gather access information	Posing as law enforcement or government officials	Digging tunnels or benches to bypass barriers	Exploting HVAC or utility access points	Hiding in seldom-used areas of the facility	Compromising administrator accounts	Using encryption to hide activities	Investigating security protocols and response times	Obtaining-data from printers or copiers	Concealing data within other files or images	Compromising data integrity or availability
Identify Vendors		Develop Cover Identity	Attempting to bypass security systems	Using social media profiles to gain trust	Disabling perimeter alarms or sensors	Using hidden compartments to smuggle tools	Setting up temporary camps or stations	Utilizing insider threats or collusion	Deploying decoys or distractions	Analyzing entry and exit logs	Collecting discarded documents from trash or recycling	Uploading data to cloud storage services	Introducing maturare or ransormulare
		Create website, ernall address, business cards, personas, and other cover documents											
Observation of site layout and security features	Continuous presence near entry and exit points	Acquiring tools and equipment for an operation	Testing physical barriers and locks	Posing as maintenance or repair personnel	Climbing fences or walls	Using stolen or counterfelt access cards	Creating hidden compartments within the facility	Using stolen or forged credentials	Disabling security cameras or alarms	Mapping out security camera locations	Gathering sensitive documents or data	Smuggling documents or data out of the facility	Destroying physical security systems or barriers
Questioning employees about sit operations	routines	Ranting or purchasing vehicles for surveillance	areas	Using fake identities to gain information	Cutting through barriers or fencing		Installing covert surveillance equipment	Exploting software vulnerabilities	Using counterfeit identification	Identifying access control points	Recording audio or video of sensitive areas	Using encrypted communication channels	Tampering with critical infrastructure
Noting security camera locations	Frequent observation of security cameras			Preferding to be a new employee	Using vehicles to ram gates or barriers	Posing as cleaning or maintenance staff	remotely accessed	Manipulating access control systems	Erosing or manipulating logs	Surveying internal tayout of the facility	Using covert cameras or recording devices	storage devices	Disrupting power or communication lines
Recording entry and exit points	Taking photographs or videos of security features	Procuring uniforms that resemble security staff	Conducting false maintenance requests	Creating fictitious scenarios to elicit information	Exploiting gaps or weaknesses in fencing	Forcing doors or windows open	Establishing redundant access points	Using social engineering to gain higher privileges	Disguising as authorized personnel		Collecting access credentials and badges	Sending data via email or file sharing senices	Initiating fire or smoke to cause evacuations
Mapping out petrol routes Observing shift changes and	Using binoculars or long-range cameras	81089	windows	Impersonating delivery or service workers	Using ladders or other tools to scale obstacles	Bypassing electronic access control systems	Using social engineering to maintain access	Installing backdoors or rooffile	Utilizing insider knowledge to avoid detection	Identifying Key personnel and their routines	Harvesting information from unlocked computers	Using remote access tools for data transfer	equipment
observing shift changes and employee routines Identifying blind spots in	Setting up hidden carrieras or recording devices  Conducting foot or vehicle patrols	Obtaining maps and blueprints of the facility Securing communication devices	Using social engineering to gather access information Attempting to bypass security	Posing as law enforcement or government officials Using social media profiles to gain	Digging tunnels or trenches to bypass barriers	Exploiting HVAC or utility access points  Usino hidden compartments to	Hiding in seldom-used areas of the facility  Setting up lamporary camps or	Compromising administrator accounts	Using encryption to hide activities	Investigating security protocols and response times	Obtaining-data from printers or copiers Collecting discarded documents	Concealing data within other files or images Uploading data to cloud storage	Compromising data integrity or availability Introducing malurare or
surveillance coverage Analyzing building schematics or	around the site	and channels  Developing escape routes and	systems Observing and testing security	trust  Calling with urgent requests for	sensors Tailgating authorized personnel	Smuggle tools  Deactivating alarm systems and	stations Compromising janiforus or utility	Utilizing insider threats or collusion Expeding default passwords or	Deploying decoys or distractions	Analyzing entry and exit logs Searching for unmonitored or	from trash or recycling Copying files from network shares	senices	ransomvare
blueprints Using drones for aerial	Using drones to monitor the facility Monitoring employee and visitor	contingency plans Cathering financial resources for	personnel reactions Testing access control systems	information Sending emails with bibricated	through gates Using take credentials to pass	sensors Cloring access basines or	closets Using false maintenance requests	settings Leveraging trust relationships between	Avoiding security patrol routes Using stealth technology or	less-secured areas Identifying locations of critical	or servers Using USB drives or other portable	exchange	controls (e.g., HVAC) Sabstaging network or IT
surveillance Monitoring delivery and service	patterns Following security personnel to	brities Assembling a team with	with take credentials Probing network or electronic	stories Prefending to be a client or	through checkpoints Sneaking through service or	Reycands Breaking through less-secured	to stay onsite Developing relationships with staff	Systems Gaining physical access to restricted	techniques Covering or altering physical	assets Scanning for wireless networks	storage devices Collecting information from public	Anneis or VPTIS Utilizing disposable or burser	infrastructure Causing physical harm to
schedules	and from the site	specialized skills	security systems Pracing objects to test security	customer	delivery entrances Exploiting maintenance or	entry points Utilizing service elevators or back	to avoid suspicion Rotating personnel to avoid	Planting malicious hardware or	appearance Disabling or tampering with	and devices Conducting dumpster diving for	displays Harvesting data from mobile	devices Transferring data over	personnel Disabling alarm systems or
Social engineering attempts to	s Using GPS trackers on vehicles Listening to radio or	Acquiring surveillance equipment Setting up decay companies or	attention Using decoy packages to test	Using fake credentials or badges Posing as contractors or	construction areas Using drones to deliver payloads	starrvays Exploiting security desk or guard	detection Establishing sleeper cells or	software	security devices Utilizing dark web or black market	discarded documents Using social engineering to gather	devices Recording keystrokes or screen	compromised network connections Using mobile devices for data	Trippering false alarms to cause
gather information identifying security weaknesses through social media	communications traffic	personas Stockpiling supplies like food and water	mailroom procedures Attempting to access sensitive areas without authorization	consultants Creating elaborate backstories for credibility	over barriers Employing decays to distract	post distractions Using insider assistance to gain	long-term presence Utilizing fake identities to regularly re-enter	Exploiting gaps in security policies Utilizing phishing attacks to gain credentials	resources Hiding in blind spots or unmonitored areas	insider information Surveying for hidden or covert security measures	captures Copying access logs or security	exitivation Sending data through hidden nativork channels	confusion  Vandalcing property or defacing surfaces
Watching for security drills and responses	Observing and noting down security response times		Conducting false deliveries to gain	Impersonating vendors or suppliers	Posing as delivery or service personnel	Disguising as high-authority personnel	Placing long-form listening devices	Compromising multi-factor	Using false credentials to avoid suspicion	Mapping out internal and external patrol routes	Collecting emails or infernal communications		Stealing critical assets or
Taking photographs of critical infrastructure	Pretending to be maintenance or delivery personnel	Building custom tools for typassing security	Observing the response to minor security breaches	Pretending to be part of the IT or security team	Timing breaches during shift changes or lew activity	Using forged documents or work orders	Using compromised IT systems for continued access		Altering or forging documents	Identifying maintenance and service schedules	Gathering data from backup or archinal systems	Using steganography to hide data	
Using binoculars or long-range cameras	Mapping out the location of all security posts			Using fake-documents to support identity claims	Utilizing natural cover (e.g., trees, bushes) to hide movements	Timing breaches during peak activity or shift changes	Employing hidden cameras or recording devices	Exploiting privilege escalation vulnerabilities	Creating fake emergency situations	Investigating physical and electronic security layers	Taking photographs of sensitive documents or screens		Manipulating safety systems (e.g., fire suppression)
Observing access control procedures	Using social media to track security schedules	Learning about security systems and technologies	Creating diversions to distract security	Calling from spoofed numbers to gain information	Creating diversions to draw security away	Placing lampered security devices to bypass checks	Manipulating security systems to avoid detection	Using brute force attacks on administrative accounts	Manipulating environmental controls (e.g., lighting)	Mapping network and communication infrastructure	Using network sniffing tools to capture data	Mailing physical copies of sensitive information	Contaminating water or air supply
Monitoring security checkpoints	Installing keyloggers on public computers	Developing cyber tools for hybrid attacks	Testing the effectiveness of surveillance carneras	Sending take invoices or purchase orders	Exploiting unmonitored areas of the perimeter	Explotting gaps in surveillance camera coverage	Creating backdoor access through software or hardware	Bypassing access control mechanisms		Identifying weaknesses in emergency procedures	Collecting data from fax machines		Causing financial loss through theft or damage
Surveying parking lot usage patients	Placing decoy items to observe response actions	Acquiring information through black market sources	Checking for unmonitored entry points	Using preferts to conduct surveillance	Using grappling hooks or ropes	Using thermal or infrared devices to navigate in the dark	Utilizing abandoned or infrequently used rooms	Compromising network infrastructure	Using secure communication channels	Analyzing public records for building schematics	Harvesting data from cloud services	Exhibiting data during shift changes or off-hours	Compromising backup or recovery systems



# Dissimilarities in Testing





CIA VS. DEATH AND CUSTOMER SERVICE



CONSEQUENCES OF GETTING CAUGHT



STAKES CAN BE HIGHER FOR PHYSICAL TESTERS



## **LESS COMMON**

- Testing is Less Common
- Adversaries are Less Commonly in Person



THIRD PARTIES ARE OFF-LIMITS



**SOCIAL ENGINEERING** 





# **Guiding** Principles

#### **LISTEN**

Talk to CSO/CISO/CTO, and whoever physical security reports to



#### **UNDERSTAND**

The business.
Where are the risks, and where would good data help with decision making?



#### **PRIORITIZE**

Based on the threat model and decisions that leadership needs to make



#### **SCOPE**

Scope the engagement to meet the company's needs, partner with physical security, and reduce risk



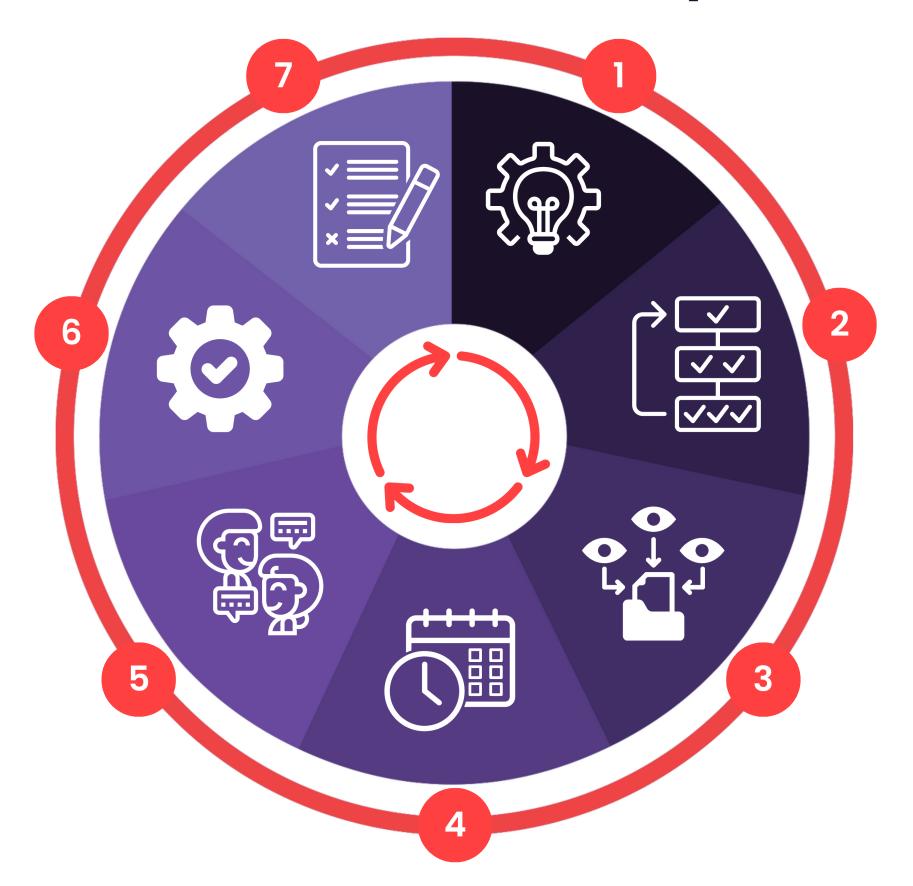
#### HELP

Ensure you're helping the blue team. You are on their side.





# Red Team LifeCycle



- 1 IDEATION
- 2 PRIORITIZATION
- 3 INTEL GATHERING
- 4 PLANNING
- 5 REHEARSAL
- 6 EXECUTION
- 7 REPORTING







Build and revisit your organization's threat model at least once a year for accuracy and relevancy

Account within it for external information only (the internal factors will come later) - this needs to be an objective resource based on true and verifiable intelligence

### Resource

**Threat Modeling Overview** 

Basic Threat Modeling Visualization:

- Standard
- Long

## 2 Ideation > Prioritization

- Poison Circles
- Stakeholder Interviews
- Insider knowledge, if permitted

Note that the specific use and extent of insider knowledge, if and when used, should be well-documented for reporting purposes (this can and will CYA on several occasions if you are anything like us).



# Prioritization > Intel-Gathering



- **OSINT**
- Research
- Internal resources

# OSINT for PhySec Red Teaming

## Building

- Blueprints
  - Tax Records for Building Owner
  - Building Manager
  - Leasing Office
  - City Records, Construction Permits
- ► 360 Tours
  - Leasing Agents
- Photos Inside
  - Tags and Geolocation



Previous RTV Talk on
OSINT for Physical
by Tim Roberts &
Brent White

## Routes In & Intel Gathering

- Find Vendors
  - Listed on their website
  - News articles
  - Purchase orders
  - Photos
  - [Surveillance / Probing]
- Find Co-Tenants
- Find Empty Floors
- Crime Maps
- Wifi (WIGLE)
- Complaints and Neighborhood Conversations
- Employees (LinkedIn)
  - Photos, Discussions, etc.



# Intel-Gathering > Planning

- Scope
- Comms
- OpSec
- Resource Acquisition
- De-Risking



### Resource

Red Team Scoping Questions

START-Physical [Under Construction]

<u>De-Risking the Red Team</u>
<u>Letter of Authorization</u>
<u>Template</u>

## De-Risking

The goal of red teams is to reduce the risk to the organization, not to increase it. Ensure tests do not cause undue risk or disruption.

## Categories or Risk:

EHS, Legal, Privacy, Compliance, GSOC, Tenant/Landlord, Firearms/Weapons, Other Risks

Key Question: Do you Notify Law Enforcement?

## **Authorization Confirmation:**

If you get caught, how do they confirm you are authorized?

LoA, Phone Numbers, Internal Post/Page, Notification of LE

Laws: Review OpsPlan against local laws

**STOPOP:** When is the operation done? What are the triggers for stopping early?



# Planning Rehearsal



- With the field info-gathering, the operators can start probing for next steps or more information as they progress.
- This new information should inform the next steps in the op.

  You receive pushback on vishing attempt but learn an additional step of the authentication process that sets you up for success for the next call.
- Rehearsal is a must for op success when using social engineering tactics, so practice vishing conversations and scenario building. But it's pivotal for physical exploits involving any danger to the operator or others, such as fence-climbing, badge-swiping, and more

## Rehearsal > Execution



Leverage all knowledge from OSINT-gathering, surveillance, and probing to make your execution a success. it's a cyclical process.

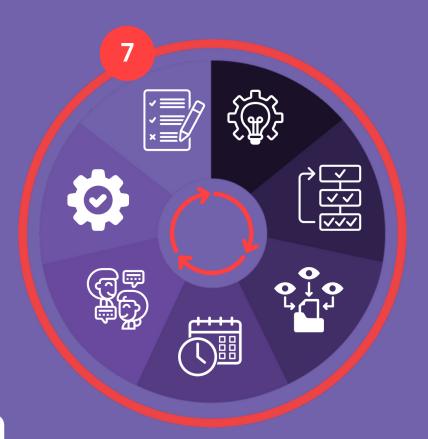
Strong communication

**Goal Focused** 

# 7 Execution > Reporting

After the execution follows the most loved portion for any operator – riveting report–writing!

It's important to remember that as a red teamer you are on the same team as the rest of the organization. Your job is to help them redirect and prioritize their remediation efforts.



## **Common Pitfalls**

## DON'T:

Cause or use uncomfortable social topics to gain entry (race, gender, etc.)

Create more risk than you mitigate

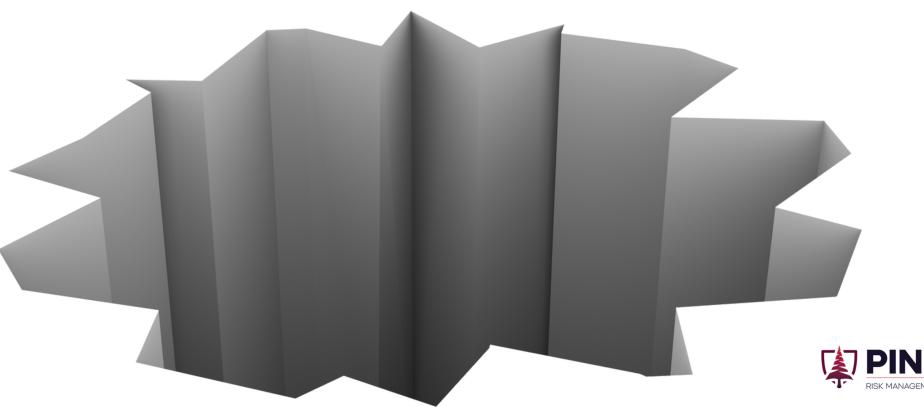
Bring your Politics to Red Teaming

Commit Crimes (you're authorized, or not)

Steamroll

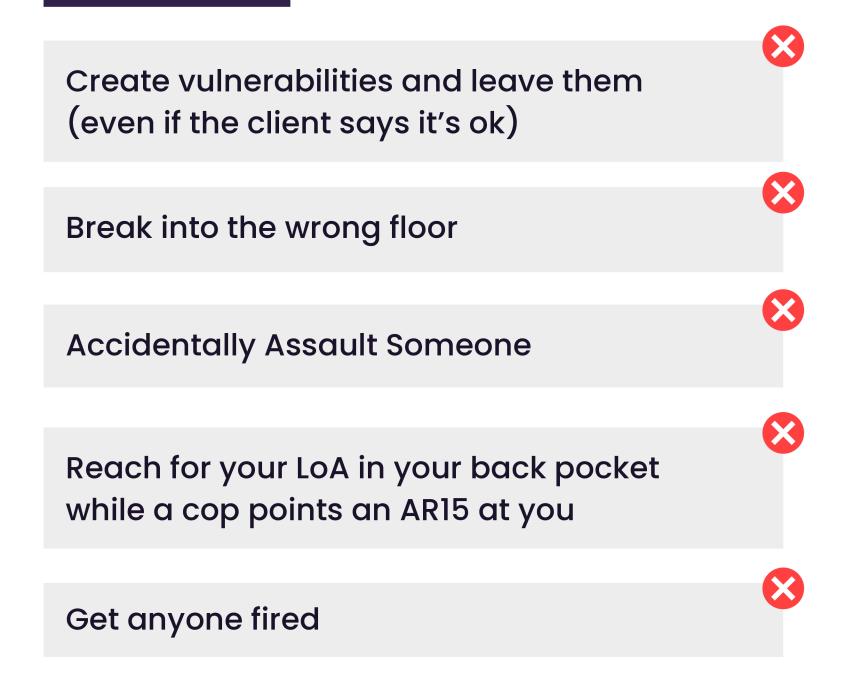
Brag (Afterward or outside of reporting chain)

Do Cowboy Shit



# The Don't of Physical Red Teaming

## DON'T:









# Bad Reasons to Conduct Physical Assessments



Political Hitjobs



Make
Department
Look Bad



**Turf-Grabs** 



Territorialness (owning "security")



Adventure Convenience Adrenaline



# Physical Red Teams Gone Wrong

- Helicopter
- Long Guns
- Special Delivery
- Fire Alarms
- Steamroller
- Tel Aviv

Resource

Physical Red Team Lessons Learned



# What makes a good physical red teamer?

## **Step 1: Fundamentals**

- The Mindset: What is red teaming?
- The basics of physical security
- Analytical Red Teaming
- Cyber Red Teaming

## **Step 3: Professional Skills**

- Systems Thinking
- Ethics & Laws
- Red Teams Gone Wrong
- Managing Red Team Risk
  - Effective Scoping
- Learning from the real Baddies (Effective Threat Modeling & Adversary Emulation)
- Security Frameworks, Standards, and Regulations
- Report Writing and Impactful Communication

## **Step 2: Technical Skills**

- Social Engineering
- OSINT
- PACS
- Bypass Techniques
  - Lockpicking

## Resource

Breaking into Red Teaming - Overview

Part 1 - Fundamentals

Part 2 - Technical Skills

<u>Part 3 - Professional Skills</u>

Physical Red Teaming Ethics Scenarios



# **Building the Team**

## PICK YOUR POISON:

Lockpicking

Social Engineering

**Impersonation** 

**OSINT** 

Bypass Techniques

RFID/PACS
Hacking

Fence Jumping

**Tailgating** 

More

You don't have to be great at any of these – just adequate. If you're testing against an advanced insider threat or counterintelligence team, you need to be great. Otherwise, be decent at half of them AND have good professional skills.



## Let's Get Physical

Seven Steps for Cyber Teams to Conduct Good Physical Assessments

#### **TALK**

Talk to the Physical **Security Teams** Early



### UNDERSTAND

**Understand their** needs, strengths, known weaknesses, goals, etc.



#### SCOPE

Focus on objectives



#### **DE-RISK**

Get **Authorization** 



### COMMUNICATE

Before, during, and after with all parties



### **DEBRIEF**

Show & Tell



#### **FRAMING**

Present, frame, and communicate your findings effectively. Know your audience. Technical terms don't work, pose it in terms of risk, threat model, and threat actors. They don't know what APTs are targeting your networks, so use the data you have to tell a compelling story.





# Collaborating with PhySec



#### **THREAT IDEATION:**

**Poison Circles** 



#### PHYSICAL-ENABLED CYBER VULNERABILITY SHARING

(If someone gets into an IDF room, X happens. If someone gets access to a LAN port on a wall in the office, Y happens). Let them know your strengths and weaknesses.

#### **JOINT OPERATIONS:**

Pull their folks into your assessment if you need a physical component



## **INFORM RISK ASSESSMENTS**



**JOINT TRAINING** 

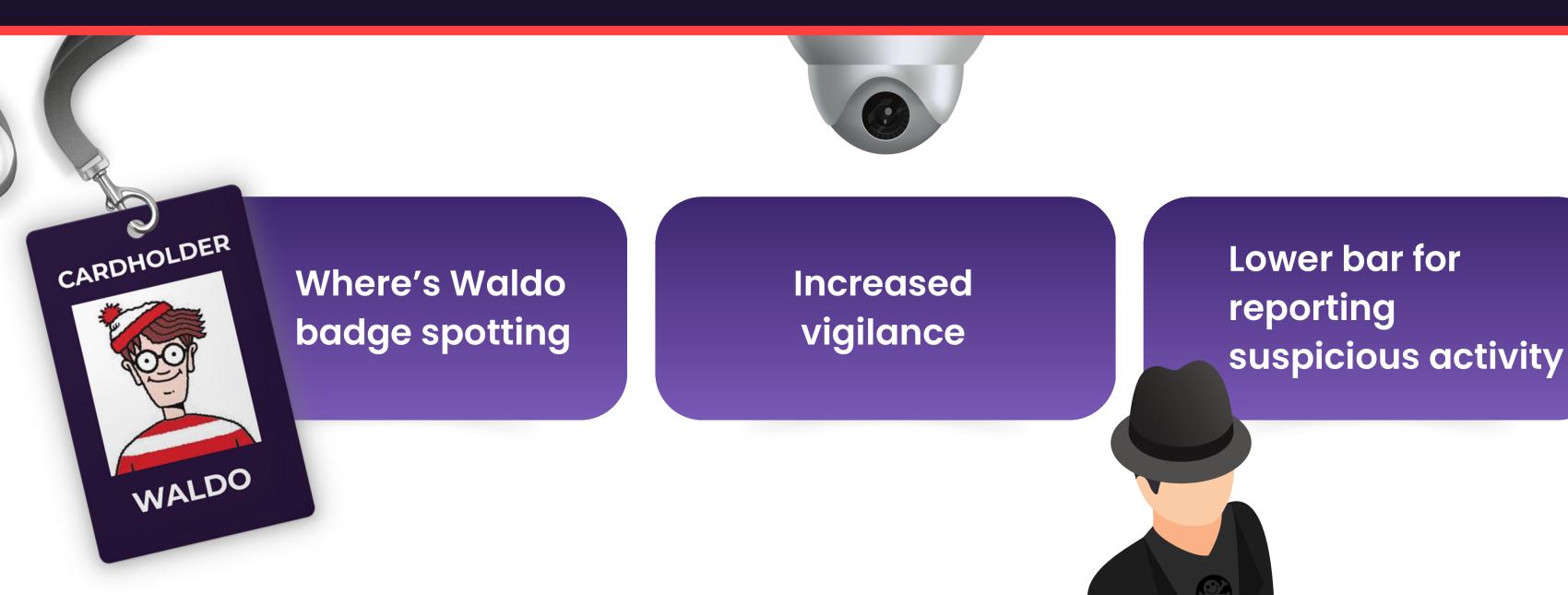


**OVERLAP** 





# Unintended Benefits of PhySec Testing



# How PRT Saves Money



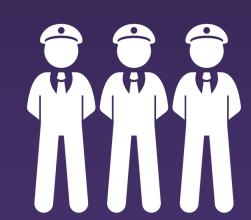


Loss Avoidance:
Avoidance of loss of assets,
negligence lawsuits, etc.

Removal of Ineffective Technology

Uncover Gaps in Vendor Implementation





Insurance - Tangible & Tested Risk Reduction

Risk Acceptance

Challenging Assumptions
Cameras in Office Space

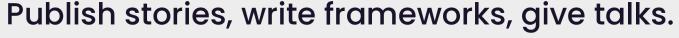


# Contribute to the Industry

Physical Security is relatively immature Physical red teaming is even less mature as a profession

## IF YOU WANT TO CONTRIBUTE:





## **Learn about Physical Security:**

Go to a conference, take a course, and translate it to Cybersecurity professionals.



Develop tools, Open Source Them.





Take effective and mature aspects of the cybersecurity and try applying them to physical security.



## Resources

## **Locks & Leaks**

locksandleaks.substack.com



## **Red Team Tools**

www.redteamtools.com



## **Resources From This Talk**

www.pinerisk.com/RTV



## **Red Team Alliance**

shop.redteamalliance.com





# Thank You!

**Get in Touch** 



Text/Call: (628) 777-7475

Signal: (952) 465-4769



Shawn@PineRisk.com Ana@PineRisk.com



Reddit.com/r/PhysicalRedTeam
Discord: ByteAbel
LinkedIn.com/Company/PineRisk

